Data Sharing and Confidentiality Requirements

Compliance with New York State Education Law Section 2-d

This Agreement is made by and between the Fredonia Central School District (the "District") and ABCya.com, LLC (the "Company"), collectively referred to herein as the "Parties." The District is an educational agency, as that term is defined in Section 2-d of the New York State Education Law ("Section 2-d"), and the Company is a third party contractor, as that term is defined in Section 2-d. The District intends to enter into this Agreement by which the Company shall have access to Student Data and/or Teacher or Principal Data regulated by Section 2-d for purposes of providing and improving the ABCya.com service.

The Company agrees to comply with the following provisions as set forth in Section 2-d prior to the District's signing of contracts and shall submit to the District a copy of its Data Security and Privacy Plan as well as the completed attached Addendum for review before final approval of this Agreement and should stay in effect for the duration of this Agreement.

A. The release by an "Educational Agency" of certain Student Data and/or Teacher or Principal Data to a "Third Party Contractor" is subject to the requirements of Section 2-d; and

B. Upon which time the Company receives, holds, or has access to Student Data and/or Teacher or Principal Data originating from the District that uses the Company's product/service pursuant to the newly-signed Agreement, the Company agrees to conform to the requirements of Section 2-d;

C. Additionally, based upon the mutual covenants and understandings between the Parties, the Parties hereby agree to the following definitions with respect to shared Student Data and/or Teacher or Principal Data, as applicable:

1. "Student Data" means personally identifiable information from student records that the Company receives or has access to from the District. "Personally Identifiable Information" ("PII") as applied to Student Data, means personally identifiable information as defined in 34 C.F.R. §99.3 implementing the Family Educational Rights and Privacy Act ("FERPA"), at 20 U.S.C. 1232g.

2. "Teacher or Principal Data" means personally identifiable information from the records of the District relating to the annual professional performance reviews of classroom teachers or principals that is confidential and not subject to release under New York State Education Law Section 3012-c.

3. "Third Party Contractor" means any person or entity, other than an educational agency, that receives Student Data and/or Teacher or Principal Data from an educational agency pursuant to a contract or other written agreement for purposes of providing services to such educational agency, including, but not limited to data management or storage services, conducting studies for or on behalf of such educational agency, or audit or evaluation of publicly funded programs.

4. "Educational Agency" means a school district, board of cooperative educational services, school, or the New York State Education Department.

5. "Parent" means a parent, legal guardian, or person in parental relation to a student.

6. "Student" means any person attending or seeking to enroll in an educational agency.

7. "Eligible Student" means a student eighteen years or older.

8. "NIST Cybersecurity Framework" means the U.S. Department of Commerce National Institute for Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity Version 1.1 which is available at the Office of Counsel, State Education Department, State Education Building, Room 148, 89 Washington Avenue, Albany, NY 12234.

9. "Unauthorized Disclosure" or "Unauthorized Release" means any disclosure or release not permitted by federal or State statute or regulation, any lawful contract or written agreement, or that does not respond to a lawful order of a court or tribunal or other lawful order.

D. Student Data and/or Teacher or Principal Data that the Company receives or has access to, including by any of its subcontractors or assignees, shall not be sold, used or disclosed for any marketing or commercial purposes.

E. The Company shall maintain the confidentiality of the Student Data and/or Teacher or Principal Data to which it has access in accordance with state and federal law and the District's data security and privacy policy.

F. The exclusive purposes for which the Company may receive or have access to Student Data and/or Teacher or Principal Data is delineated in the Underlying Contract. The Company agrees to not use the Student Data and/or Teacher or Principal Data for any other purposes.

G. The Company further agrees that it will protect the confidentiality, privacy and security of Student Data and/or Teacher or Principal Data in accordance with the District's Parents Bill of Rights for Data Privacy and Security ("Bill of Rights"). A copy of the Bill of Rights is attached hereto as **Appendix A.**

H. The Company agrees that any of its officers or employees, and any officers or employees of any subcontractor or assignee of the Company, who may be granted access to the Student Data and/or Teacher or Principal Data, have received or will receive training on the federal and state law governing confidentiality of such data prior to receiving the data or access to the data.

I. The Company acknowledges that as a "Third Party Contractor" of the District, it has certain statutory and regulatory obligations under Section 2-d with respect to Student

Data and/or Teacher or Principal Data, and agrees that failure to fulfill one or more of these statutory and/or regulatory obligations shall be deemed a breach of both the Underlying Contract and this Agreement:

1. To adopt technologies, safeguards and practices that align with the NIST Cybersecurity Framework;

2. To comply with the District's data security and privacy policy; Section 2-d and its corresponding regulations;

3. To limit internal access to education records and shared Student Data and/or Teacher or Principal Data to those individuals that are determined to have legitimate educational interests within the meaning of Section 2-d and the Family Educational Rights and Privacy Act (FERPA) (*i.e.,* the individual needs access to the Student Data and/or Teacher or Principal Data in order to provide the contracted services);

4. To not use student education records or shared Student Data and/or Teacher or Principal Data for any purpose not explicitly authorized in this Agreement or Underlying Contract;

5. To not disclose any personally identifiable information to any other party who is not an authorized representative of the Company using the information to carry out the Company's obligations under the Underlying Contract, unless:

    a. the parent or eligible student has provided prior written consent; or

    b. the disclosure is required by statute or court order, and notice of the disclosure is provided to the District no later than the time of disclosure, unless such notice is expressly prohibited by the statute or court order;

6. To maintain reasonable administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of personally identifiable information in its custody; and

7. To use encryption technology to protect personally identifiable information while in motion or in its custody from unauthorized disclosure using a technology or methodology specified by the Secretary of the United States Department of Health and Human Services in guidance issued under Section 13402(H)(2) of Public Law 111-5.

J. The Company further acknowledges the following additional obligations under Section 2-d regarding breach and unauthorized release of Student Data and/or Teacher or Principal Data, and agrees that failure to fulfill one or more of these additional statutory obligations shall be deemed a breach of both the Underlying Contract and this Agreement:

1. To promptly notify the District of any breach of security resulting in an unauthorized release of personally identifiable data by the Company or its subcontractors or assignees in violation of applicable state or federal law, the District's Parents Bill of Rights set forth in **Appendix A** of this Agreement, or obligations relating to data privacy and security contained within this Agreement, in the most expedient way possible and without unreasonable delay, but no more than seven (7) calendar days after the discovery of such breach.

2. The Company must cooperate with the District and law enforcement to protect the integrity of investigations into the break or unauthorized release of personally identifiable information.

3. In the event that the District is required under Section 2-d to notify affected parent(s), student(s), eligible student(s), teacher(s) and/or principal(s) of an unauthorized release of Student Data and/or Teacher or Principal Data by the Company or its assignees or subcontractors, the Company shall promptly reimburse the District for the full cost of such notification.

K. The Company will ensure that any subcontractors or assignees with whom it shares Student Data and/or Teacher or Principal Data will abide by the data protection and security requirements of Section 2-d, by requiring them to execute written agreements which subject them to the terms of this Agreement.

L. Upon expiration of this Agreement without a successor Agreement in place, the Company shall assist the District in exporting all Student Data and/or Teacher or Principal Data previously received by the Company, if any, back to the District. The Company shall thereafter securely delete any and all data remaining in the Company's possession or its assignees or subcontractors (including all hard copies, archived copies, electronic versions or electronic imaging of hard copies of shared data) as well as any and all data maintained on behalf of the Company in secure data center facilities within ten (10) days of termination of services, and provide confirmation of same to the District. The Company shall ensure that no copy, summary or extract of the data or any related work papers are retained on any storage medium whatsoever by the Company, its subcontractors or assignees, or the aforementioned secure data center facilities. To the extent that the Company and/or its subcontractors or assignees may continue to be in possession of any de-identified data (data that has had all direct and indirect identifiers removed), they agree not to attempt to re-identify de-identified data and not to transfer de-identified data to any party. Upon request, the Company and/or its subcontractors or assignees will provide a certification to the District from an appropriate officer that the requirements of this paragraph have been satisfied in full.

M. In the event that a parent, student, eligible student, teacher or principal wishes to challenge the accuracy of the data concerning that student, eligible student, teacher or principal that was shared with the Company and is maintained by or under the control of the Company, that challenge shall be processed through the procedures provided by the student's school district of residence for amendment of education records under FERPA.

The Company will be notified by the District of the outcome of any such challenges and will promptly correct any inaccurate data it or its subcontractors or assignees maintain.

N. Student Data and/or Teacher or Principal Data transferred to the Company by the District will be stored in electronic format on systems maintained by or under the direct control of the Company in a secure data center facility, or a data facility maintained by a New York board of cooperative educational services, within the United States. The measures that the Company will take to protect the privacy and security of the Student Data and/or Teacher or Principal Data while it is stored in this manner shall be those associated with industry best practices including, but not necessarily limited to, disk encryption, file encryption, firewalls, and password protection.

O. The Company hereby acknowledges that it may be subjected to civil penalties for failure to property protect and secure student, teacher or principal data, as outlined in Section 2-d.

P. To the extent that any term of the Underlying Contract conflicts with the terms of this Agreement, the terms of this Agreement shall apply and be given effect. In the event that the Company has Terms of Service (TOS) that may otherwise be applicable to its customers or users of its product/service, to the extent that any term of such TOS conflicts with the terms of this Agreement, the terms of this Agreement shall apply and be given effect.

Q. Any revisions to this Agreement shall be by mutual written agreement of the Parties. Notwithstanding the foregoing, the Parties acknowledge that modifications to this Agreement may be necessary in the future to ensure compliance with Section 2-d and its applicable regulations, issuance of further guidance by the New York State Education Department, and the District's Policy on data security and privacy subsequent to the Parties' execution of this Agreement. Necessary modifications at that time will include incorporation into this Agreement of the Company's data security and privacy plan that will outline how all state, federal, and local data security and privacy contract requirements will be implemented over the life of the contract, consistent with the District's Policy on data security and privacy. The Parties agree to act in good faith to take such additional steps as may be necessary at that time.

Agreed on this ___ day of January, 2024.

VENDOR:
Print: Paul Mishkin
Sign: _____
Date: 1/23/2024

DISTRICT:
Print: Andrew M. Wheelock
Sign: _____
Date: 1/23/2024

AP PENDIX A
Parents' Bill of Rights for Data Privacy and Security

The Fredonia Central School District is committed to protecting the privacy and security of student, teacher, and principal data. In accordance with New York Educational Law §2-d, the District wishes to inform the school community of the following:

1. A student's personally identifiable information cannot be sold or released for any commercial purposes.
2. Parents have the right to inspect and review the complete contents of their child's education record.
3. State and federal laws protect the confidentiality of personally identifiable information, and safeguards associated with industry standards and best practices, including but not limited to, encryption, firewalls, and password protection, must be in place when data is stored or transferred.
4. A complete list of all student data elements collected by the State is available for public review at: http://www.p12.nysed.gov/irs/sirs/documentation/NYSEDstudentDATA.xlsx, or by writing to the Office of Information & Reporting Services, New York State Education Department, Room 863 EBA, 89 Washington Avenue, Albany, New York 12234.
5. Parents have the right to have complaints about possible breaches of student data addressed. Complaints should be directed in writing to Temitope Akinyemi, the Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, New York 12234.

Supplemental Information Regarding Third-Party Contractors

In the course of complying with its obligations under the law and providing educational services to District residents, the Fredonia Central School District enters into agreements with certain third-party contractors. Pursuant to such agreements, third-party contractors may have access to "student data" and/or "teacher or principal data," as those terms are defined by law.
Each contract the District enters into with a third party contractor where the third party contractor receives student data or teacher or principal data will include the following information:

1. The exclusive purposes for which the student data or teacher or principal data will be used;
2. How the third party contractor will ensure that the subcontractors, persons or entities that the third party contractor will share the student data or teacher or principal data with, if any, will abide by data protection and security requirements;
3. When the agreement expires and what happens to the student data or teacher or principal data upon expiration of the agreement;
4. If and how a parent, student, eligible student, teacher or principal may challenge the accuracy of the student data or teacher or principal data that is collected; and

Where the student data or teacher or principal data will be stored (described in such a manner as to protect data security), and the security protections taken to ensure such data will be protected, including whether such data will be encrypted.

ADDENDUM – SUPPLEMENTAL INFORMATION

The supplemental information obtained below will be included with the Fredonia Central School District's (the "District") Parents' Bill of Rights as required by New York State Education Law Section 2-d [3][c]. The Parents' Bill of Rights and this supplemental information may be redacted to the extent necessary to safeguard the privacy and/or security of the District's data and/or technology infrastructure.

1. The Company agrees to use Student Data and/or Teacher or Principal Data for the exclusive purposes listed below:

To provide the ABCya.com Service as set forth in the ABCya.com Terms of Use (www.abcya.com/terms/. Student data, teacher or principal data will not be used for any other purpose.

2. The Company will provide to the District, in writing, a statement indicating how it will ensure that any subcontractors, or other authorized persons or entities to whom the Company will disclose such Student Data and/or Teacher or Principal Data, if any, will abide by data protection and security requirements, including, but not limited to, those outlined in applicable state and federal laws and regulations (e.g., FERPA, Education Law Section 2-d):

ABCya.com seeks out service providers that shares their commitment to maintaining the privacy and security of Personal Data and requires their subprocessors to respect their user data to the same or greater degree as they do. Education.com has implemented a variety of physical, administrative and technological safeguards designed to preserve the integrity and security of the personal information they collect and to protect against unauthorized access to data. These include internal reviews of their data collection, storage, and processing practices and security measures, as well as physical security measures to guard against unauthorized access to systems where they store personal data. ABCya.com restricts access to personal information to their employees, contractors, and agents who need to know that information in order to operate, develop, or improve their services.

3. The Company will provide the District with a written description of what will happen to Student Data and/or Teacher or Principal Data upon expiration of this Agreement or other written agreement (e.g., whether, when, and in what format data will be returned to the District, and/or whether, when, and how the data will be destroyed).

Unless otherwise directed by a School or Parent, ABCya.com will delete or de-identify personal information of student and child users after a period of inactivity, after the termination or cancellation of the license subscription, or after termination of our agreement with the School, in accordance with the terms of any applicable written agreement with the School, written requests from authorized School administrators, and our standard data retention schedule.

4. The Company will provide the District with a written description of how a parent, student, eligible student, teacher or principal may challenge the accuracy of the Student Data and/or Teacher or Principal Data that is collected.

Parents, students, eligible students, and teachers or principals may contact their School to exercise this right. ABCya.com will cooperate with the School to effectuate such requests at the School's discretion.

5. The Company will provide the District with a written description of where the Student Data and/or Teacher or Principal Data will be stored (described in such a manner as to protect data security), and the security protections taken to ensure that such data will be protected, including, how such data will be protected using encryption while in motion and at rest.

Data is stored in the United States. As outlined herein, ABCya.com's practices are designed and implemented with the goal of maximizing the security and privacy of all customer data. This includes limiting access to EA data to employees with a business need and encrypting all data in transit and at rest. ABCya.com will use reasonable administrative, technical and physical safeguards that align with the NIST Cybersecurity Framework and are otherwise consistent with industry standards and best practices, including but not limited to: encryption, firewalls, and password protection as specified by the Secretary of the United States Department of HHS in any guidance issued under P.L. 111-5, Section 13402(H)(2), to protect the security, confidentiality and integrity of student data of the District while in motion or in custody of Department from unauthorized disclosure.